

#3

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

JCS62 U.S. PRO  
09/733912  
12/12/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出 願 年 月 日

Date of Application:

2000年 6月29日

願 番 号

Application Number:

特願2000-196040

願 人

Applicant (s):

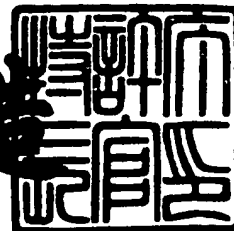
富士通株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年 9月22日

特許庁長官  
Commissioner,  
Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 0051220

【提出日】 平成12年 6月29日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 9/00  
G09C 1/00

【発明の名称】 暗号制御装置

【請求項の数】 5

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 関 裕二

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 川崎 雄介

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 橋本 繁

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 柳 良一

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100094330

【弁理士】

【氏名又は名称】 山田 正紀

【選任した代理人】

【識別番号】 100109689

【弁理士】

【氏名又は名称】 三上 結

【手数料の表示】

【予納台帳番号】 017961

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9912909

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号制御装置

【特許請求の範囲】

【請求項 1】 プログラムを実行する CPU と、該 CPU で実行されるプログラムが格納された ROM と、該 CPU でのプログラム実行中の作業領域として使用される RAM と、外部機器との間のデータの送受信を担う I/O 部と、暗号化されたデータの復号化および平文のデータの暗号化を担う暗号部とが 1 つの半導体素子上に形成されてなることを特徴とする暗号制御装置。

【請求項 2】 前記 RAM が、暗号化されたデータを復号化するための秘密鍵を格納してなるものであり、

前記 ROM が、この暗号制御装置を使用する正当な権原を有する者を特定するデータを格納してなるものであって、

この暗号制御装置は、外部からデータが送信されてくるのを待つ待機モードと、動作が可能な動作可能モードとを有し、待機モードにあるときに外部から送信されてきた暗号化されたデータを前記 RAM に格納されている秘密鍵で復号化して平文のデータを生成し、該平文のデータと前記 ROM に格納されてなるデータとを照合し、これらのデータが符合するか否かに応じて、それぞれ、動作可能モードに移行し、あるいは待機モードに戻るモード切換手段を有することを特徴とする請求項 1 記載の暗号制御装置。

【請求項 3】 前記 ROM は、前記動作可能モードで実行される複数のメインプログラムを格納してなるものであり、

この暗号制御装置は、前記待機モードにあるときに外部から送信されてきたデータに基づいて、前記動作可能モードで動作させる、前記複数のメインプログラムのうちのいずれか 1 つのメインプログラムを選択するメインプログラム選択手段を有することを特徴とする請求項 2 記載の暗号制御装置。

【請求項 4】 前記 1 つの半導体素子がさらに、この暗号制御装置との間で送受信されるデータに基づく情報処理を行なう外部の情報処理装置との間のデータの送受信を担うとともにデータを送信してきた者が正当な権原を有するものであるか否かを認証する認証部を搭載してなるものであることを特徴とする請求項

1 記載の暗号制御装置。

【請求項 5】 データの暗号化、復号化に用いる鍵を生成する鍵生成手段を有し、この暗号制御装置は、該鍵生成手段で生成された鍵を用いてデータの暗号化および復号化を行なうものであることを特徴とする請求項 1 記載の暗号制御装置。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、データの暗号化や復号化を担う暗号制御装置に関する。

【 0 0 0 2 】

【従来の技術】

近年の通信技術の発達により、電子マネー等、金券と同等の価値を持つデータが行き交うようになってきており、データの不正な漏洩やデータの改ざんをどのように防止するかが極めて重要になってきている。

【 0 0 0 3 】

このようなデータの安全対策の 1 つとして、データを暗号化して送り、受信側で受け取ったデータを復号化するという、データの暗号化、復号化という手法が用いられている。このデータの暗号化や復号化には、従来、パーソナルコンピュータ（以下、P C と略記することがある）等の汎用の情報処理装置が使用されている。

【 0 0 0 4 】

また、電子マネー等を取り扱うシステムの典型例として近年 I C カードを用いるシステムが注目されているが、I C カードをアクセスする I C カードリーダー等の周辺機を制御する I / O 制御装置としては、従来、複数の半導体素子からなる I / O 制御装置が使用されている。

【 0 0 0 5 】

【発明が解決しようとする課題】

汎用の情報処理装置を使用して暗号、復号演算を行なう場合、暗号、復号のアルゴリズムやその暗号、復号に用いる鍵の秘匿が難しく、それらのアルゴリズム

や鍵が不正に漏洩し、データの改ざん等を許すという結果をもらすおそれがある。

【 0 0 0 6 】

また、ＩＣカードリーダーライタ等の周辺機を制御するＩ／Ｏ制御装置は、従来、複数の半導体素子で構成されているため、それらの半導体素子間をつなぐアドレスバスやデータバス上にＩ／Ｏ制御の途中経過の情報が出力されることになり、その情報が不正に盗まれるおそれがある。

【 0 0 0 7 】

このように従来は、まだまだデータの安全性に問題があり、その安全性を一層向上させることが求められている。

【 0 0 0 8 】

本発明は、上記事情に鑑み、データの安全性が一層向上した暗号制御装置を提供することを目的とする。

【 0 0 0 9 】

【課題を解決するための手段】

上記の課題を達成する本発明の暗号制御装置は、プログラムを実行するＣＰＵと、そのＣＰＵで実行されるプログラムが格納されたＲＯＭと、そのＣＰＵでのプログラム実行中の作業領域として使用されるＲＡＭと、外部機器との間のデータの送受信を担うＩ／Ｏ部と、暗号化されたデータの復号化および平文のデータの暗号化を担う暗号部とが１つの半導体素子上に形成されてなることを特徴とする。

【 0 0 1 0 】

本発明の暗号制御装置は、上記の各要素が１つの半導体素子上に搭載されているため、アドレスバスやデータバス上の情報を外部に出力する必要がなく、暗号化、復号化の処理の推測が困難である。

【 0 0 1 1 】

ここで、上記本発明の暗号制御装置は、

上記ＲＡＭが、暗号化されたデータを復号化するための秘密鍵を格納してなるものであり、

上記ＲＯＭが、この暗号制御装置を使用する正当な権原を有する者を特定する

データを格納してなるものであって、

この暗号制御装置は、外部からデータが送信されてくるのを待つ待機モードと、動作が可能な動作可能モードとを有し、待機モードにあるときに外部から送信されてきた暗号化されたデータを上記RAMに格納されている秘密鍵で復号化して平文のデータを生成し、その平文のデータと上記ROMに格納されてなるデータとを照合し、これらのデータが符合するか否かに応じて、それぞれ、動作可能モードに移行し、あるいは待機モードに戻るモード切換手段を有することが好ましい。

【 0 0 1 2 】

このような照合を行なうことによって不正なアクセスを防止することができ、また、特に動作する必要のないときは待機モードにあって unnecessary 電力消費を抑えることができる。

【 0 0 1 3 】

また、この場合に、上記ROMは、上記動作可能モードで実行される複数のメインプログラムを格納してなるものであり、

この暗号制御装置は、上記待機モードにあるときに外部から送信されてきたデータに基づいて、上記動作可能モードで動作させる、上記複数のメインプログラムのうちのいずれか1つのメインプログラムを選択するメインプログラム選択手段を有することが好ましい。

【 0 0 1 4 】

このように複数のメインプログラムをROM内に格納しておくことにより、この暗号制御装置を様々の用途に適用することができ、また動作可能なメインプログラムを待機モードから動作可能モードに移るときに1つだけ選択することにより、複数のメインプログラムどうしの干渉を避け、データの安全性、処理の確実性が保たれる。

【 0 0 1 5 】

また、上記本発明の暗号制御装置において、上記1つの半導体素子がさらに、この暗号制御装置との間で送受信されるデータに基づく情報処理を行なう外部の情報処理装置との間のデータの送受信を担うとともにデータを送信してきた者が

正当な権原を有するものであるか否かを認証する認証部を搭載してなるものであることが好ましい。

【 0 0 1 6 】

1つの半導体素子内にさらに上記のような認証部を搭載すると、認証により外部の情報処理装置との間で送受信されるデータの安全性が保たれる。また、専用の認証部を備えることにより、CPUでのソフトウェア動作による認証と比べ認証処理の高速化が図られる。

【 0 0 1 7 】

また、本発明において、データの暗号化、復号化に用いる鍵を生成する鍵生成手段を有し、この暗号制御装置は、その鍵生成手段で生成された鍵を用いてデータの暗号化および復号化を行なうものであることが好ましく、この場合に上記鍵生成手段は、秘密鍵と公開鍵とを生成し、公開鍵のみ外部に送信し、秘密鍵は上記RAMに格納するものであることが好ましい。

【 0 0 1 8 】

こうすることにより、秘密鍵の秘守性、安全性が保たれ、データの不正な解読が一層困難となる。

【 0 0 1 9 】

また、上記の認証部を備えた構成において、

上記RAMが、暗号化されたデータを復号化するための秘密鍵を格納してなるものであり、

上記ROMが、この暗号制御装置を使用する正当な権原を有する者を特定するデータを格納してなるものであって、

上記認証部で受信された暗号化されたデータを上記RAMに格納されている秘密鍵で復号化して平文のデータを生成し、その平文のデータと上記ROMに格納されてなるデータとを照合し、これらのデータが符合した場合に限り、上記I/O部を動作可能とするI/O部制御手段を有することが好ましく、

この場合に、上記1つの半導体素子が、上記I/O部を複数搭載してなるものであって、上記I/O部制御手段は、上記認証部で受信されたデータに基づいて、そのデータに応じたI/O部のみ動作可能とするものであることも好ましい形



態であり、

あるいは、上記 I / O 部は、複数のセキュリティレベルのうちの任意のセキュリティレベルの設定が自在なものであり、上記 I / O 部制御手段は、上記認証部で受信されたデータに基づいて、上記 I / O 部を、そのデータに応じたセキュリティレベルに設定するものであることも好ましい形態である。

【 0 0 2 0 】

このような照合を行なうことによって不正なアクセスを防止することができる。また、必要な場合のみ I / O 部を動作可能とすることが一層の安全性を確保する上で有用であるとともに省電力化を図ることもできる。さらに、上記のようにセキュリティレベルを制御することで、不必要のアクセスの防止を図り、安全性を一層向上させることができる。

【 0 0 2 1 】

また、上記の認証部を備えた構成において、その認証部は、外部の情報処理装置との間のデータの送受信を、モデムを介して行なうものであることも好ましい形態である。

【 0 0 2 2 】

この場合、離れた場所から暗号制御装置の動作を開始させることができる。

【 0 0 2 3 】

さらに、本発明の暗号制御装置において、異常の検知を受けて、上記 R A M に格納されているデータを破壊するデータ破壊手段を有することが好ましい。

【 0 0 2 4 】

こうすることにより鍵が不正な侵入者に渡るのを防止することができる。

【 0 0 2 5 】

【発明の実施の形態】

以下、本発明の実施形態について説明する。

【 0 0 2 6 】

図 1 は、本発明の暗号制御装置の第 1 実施形態を示すブロック図である。

【 0 0 2 7 】

この暗号制御装置 1 0 A は、1 つの半導体素子 1 0 0 A 内に形成されており、

この暗号制御装置 1 0 A は、プログラムを実行する CPU 1 1 A、CPU 1 1 A でのプログラム実行中の作業領域として使用される RAM 1 2 A、CPU 1 1 A で実行されるプログラムが格納された ROM 1 3 A、外部機器（ここでは IC カードリーダーライタ（IC カード R/W）2 0 0）との間でデータを送受信する I/O 部 1 4 A、および、暗号化されたデータの復号化や平文のデータの暗号化を担う暗号部 1 5 A から構成されている。この暗号制御装置 1 0 A を構成する各要素は、内部バス 2 0 A で相互に接続されている。

## 【 0 0 2 8 】

ROM 1 3 A には暗号処理アルゴリズムや I/O 部 1 4 A を制御するプログラムなどが含まれている。

## 【 0 0 2 9 】

また、IC カード R/W 2 0 0 と I/O 部 1 4 A との間で送受信されるデータには、IC カード R/W 2 0 0 を制御する制御データ、および IC カードから読み出した暗号データがある。IC カードから読み出されるデータはその IC カードの機能によって暗号化されてからその IC カードから読み出され、IC カード R/W 2 0 0 から暗号制御装置 1 0 A に送られる。暗号制御装置 1 0 A に送られた暗号データはその暗号制御装置 1 0 A の暗号部 1 5 A によって復号化される。一方、暗号制御装置 1 0 A 内で生成された、IC カードへの送信用のデータは、その暗号制御装置 1 0 A の暗号部 1 5 A によって暗号化され、I/O 部 1 4 A を経由して IC カード R/W 2 0 0 に送られ、その IC カード R/W 2 0 0 に挿入されている IC カードに書込まれる。IC カード内ではその IC カードの機能によってその暗号データが復号化される。

## 【 0 0 3 0 】

このような構成を採ることで、暗号部 1 5 A と RAM 1 2 A、ROM 1 3 A との間でやりとりされるデータは一切外部に漏れず、セキュリティの高い暗号制御装置が構築される。

## 【 0 0 3 1 】

図 2 は、本発明の暗号制御装置の第 2 実施形態を示すブロック図、図 3 は、図 2 に示す第 2 実施形態における動作フローチャートである。

## 【 0 0 3 2 】

この暗号制御装置 1 0 B は、1 つの半導体素子 1 0 0 B 内に形成されている。この暗号制御装置 1 0 B は、CPU 1 1 B、RAM 1 2 B、ROM 1 3 B、暗号部 1 5 B、およびインタフェース部 1 6 B から構成されている。これらのうち、CPU 1 1 B、RAM 1 2 B、ROM 1 3 B、および暗号部 1 5 B は、図 1 に示す第 1 実施形態の暗号制御装置 1 0 A の、CPU 1 1 A、RAM 1 2 A、ROM 1 3 A、および暗号部 1 5 A とそれぞれ同じ要素であり、重複説明は省略する。

## 【 0 0 3 3 】

また、インタフェース部 1 6 B は、図 1 に示す暗号制御装置 1 0 A の I / O 部 1 4 A に相当する構成要素であるが、図 1 の I / O 部 1 4 A は、IC カード R / W 2 0 0 との間のデータ送受信に適合したものであるのに対し、この図 2 に示すインタフェース部 1 6 B は、パーソナルコンピュータ (PC) 3 0 0 の I S A バスに接続され、PC 3 0 0 との間で I S A バスを介してデータの送受信を行なうのに適合した構成となっている。

## 【 0 0 3 4 】

図 3 に示す動作フローは、暗号制御装置 1 0 B に電源が投入されたパワーオン (PON) 時に起動されるものである。パワーオンで図 3 のスタートアップルーチンが起動されると、先ず暗号制御装置 1 0 B の最小限の初期化処理が行なわれ (ステップ a 1)、PC 3 0 0 からの情報入力待機状態となる (ステップ a 2)。この待機状態は、PC 3 0 0 からの情報が入力されたときに入力されたことを検知する部分のみ動作し、他の部分は動作しない状態にあり、電力の消費が抑えられている。

## 【 0 0 3 5 】

PC 3 0 0 から送信されてくる情報は暗号化されており、PC 3 0 0 から送信されてきた情報を受け取るとその情報の復号処理が行なわれる (ステップ a 3)。この復号処理は、RAM 1 2 B にあらかじめ格納されている秘密鍵を用いて行なわれる。この段階では暗号部 1 5 B は未だ動作不能状態のままになっており、したがってこのときは暗号部 1 5 B は使用されず、ROM 1 3 B に格納されているプログラムによりソフトウェア上で復号処理が行なわれる。

## 【 0 0 3 6 】

この待機状態において P C 3 0 0 から入力される情報には I D やパスワードが含まれており、復号された情報と、あらかじめ R O M 1 3 B に格納されている情報とを照合することにより、この暗号制御装置 1 0 B を使用する正当な権原を有する者から受け取った情報であるか否かの情報確認が行なわれ（ステップ a 4）、正当な権原を有する者からの情報ではないと判定されるときは、ステップ a 2 に戻り、P C からの情報入力待機状態に戻る。

## 【 0 0 3 7 】

一方、ステップ a 4 で、正当な権原を有する者からの情報であると判定されたときは、暗号制御装置 1 0 B の各部の初期化設定処理を行ない（ステップ a 5）、メインルーチンコールを行なう（ステップ a 6）。その後、メインルーチンが実行される（ステップ a 7）。

## 【 0 0 3 8 】

このように、本実施形態の暗号制御装置は、P C からの要請があるまでは待機状態にあり、無駄な電力消費が抑制されている。

## 【 0 0 3 9 】

図 4 は、本発明の暗号制御装置の第 3 実施形態における、R O M 内部のプログラムの構造を示した模式図である。

## 【 0 0 4 0 】

この第 3 実施形態の暗号制御装置の構成自体は、図 2 に示すものと同じであり、図 2 を参照することとし、ここでの重複した図面の提示は省略する。

## 【 0 0 4 1 】

R O M 1 3 B に格納されたプログラムは、スタートアップルーチンと、メインルーチン振分けルーチンと、3 つのメインルーチン A、B、C とから構成されている。各メインルーチン A、B、C は、それぞれ対応した情報 A、B、C についてのみ参照することができる。メインルーチン A、B、C は、暗号、復号の制御アルゴリズムが相互に異なる一つの暗号制御装置についてタイプの異なる使い方を可能としている。

## 【 0 0 4 2 】

図 5 は、図 4 にプログラム構造を示す第 3 実施形態における動作フローを示すフローチャートである。

【 0 0 4 3 】

図 5 に示す動作フローは、図 3 に示す動作フローの場合と同様、暗号制御装置 1 0 B に電源が投入されたパワーオン（P O N）時に起動されるものであり、このパワーオンでは、図 4 プログラム構造中スタートアップルーチンが起動される。

【 0 0 4 4 】

この図 5 に示す動作フローにおけるステップ b 1 ～ b 5 は、それぞれ図 3 に示す動作フローのステップ a 1 ～ a 5 とそれぞれ同一であり、重複説明は省略する。

【 0 0 4 5 】

ステップ b 6 では、ステップ b 2 で受け取りステップ b 3 で復号処理の行なわれた情報に基づいて 3 つのメインルーチン A、B、C のうちのいずれのメインルーチンを動作させるかが決定され、決定されたメインルーチンについて（ステップ b 7、b 8）、内部の初期設定（ステップ b 9、b 1 0 又は b 1 1）およびメインプログラムの実行（ステップ b 1 2、b 1 3 又は b 1 4）が行なわれる。

【 0 0 4 6 】

このように、ROM 内に複数のメインプログラムを格納しておき、待機状態から立ち上がるときに選択的にいずれか 1 つのメインプログラムのみ動作可能とすることで、様々な用途に適合させることができるとともに、メインプログラムどうしの干渉を避け、データの安全性、処理の確実性が保たれる。

【 0 0 4 7 】

図 6 は、本発明の暗号制御装置の第 4 実施形態を示すブロック図である。

【 0 0 4 8 】

この暗号制御装置 1 0 C は、1 つの半導体素子 1 0 0 C 内に形成されたものであり、CPU 1 1 C、RAM 1 2 C、ROM 1 3 C、I/O 部 1 4 C、および暗号部 1 5 C は、図 1 に示す第 1 実施形態の暗号制御装置 1 0 A の、対応する各要素とそれぞれ同一であり、重複説明は省略する。尚、この図 6 では、RAM 1 2

Cに鍵が格納されていることが模式的に明示されている。

【 0 0 4 9 】

また、図6の暗号制御装置10Cを構成する認証部16Cは、PC300と接続されてそのPC300との間でシリアルデータの送受信を行なうインタフェースであるとともに、データを送信してきた者が正当な権原を有する者であるか否かを認証するという役割りを担っている。

【 0 0 5 0 】

図7は、PC300から暗号制御装置10Cに向けて送信される認証データのデータ構造を示す図である。

【 0 0 5 1 】

PC300から暗号制御装置10Cへは、そのPC300のユーザを特定するIDおよびパスワードと、I/O部14Cを制御するための情報であるI/O情報が含まれており、この認証データは、暗号制御装置10Cの暗号部15Cで前もって作成され認証部16Cを経由して受け取っている公開鍵（以下に説明する図8に示す公開鍵0）で暗号化されたものである。

【 0 0 5 2 】

図8は、PC300と暗号制御装置10Cとの間での認証の手順を示した図である。

【 0 0 5 3 】

まず、暗号制御装置では前もって秘密鍵1と公開鍵0を生成し公開鍵0がPCに渡されている。秘密鍵は、暗号制御装置10CのRAM12Cに格納しておき、決して外部には出さないようにしておく。この公開鍵0を用いて暗号化されたデータは、秘密鍵1を用いてのみ復号化することができる。

【 0 0 5 4 】

PCでは、暗号制御装置との間でデータの送受信を行なうとしたとき、まず、図7に示すデータ形式の認証データを作成し、その認証データを、あらかじめ暗号制御装置から受け取っている公開鍵0で暗号化して暗号制御装置に送る。

【 0 0 5 5 】

暗号制御装置は、この暗号化された認証データを受け取ると、RAM12Cに

あらかじめ格納しておいた秘密鍵 1 を用いてその認証データを復号化して平文の認証データを生成する。尚、この認証データの受信の際は、この暗号制御装置は待機状態にあり必要最小限の要素のみ動作し、例えば図 6 に示す I / O 部 1 4 C や復号部 1 5 C は非動作状態にあり、したがってこの認証データの復号化は R O M 1 3 C に格納されている復号化プログラムによりソフトウェア的に行なわれる。

## 【 0 0 5 6 】

暗号制御装置では、この復号化された認証データを秘密鍵 1 で復号化して平文の認証データを生成した後、その生成した平文の認証データが R O M 1 3 にあらかじめ格納しておいた照合用の認証データと照合される。この照合により双方の認証データが一致したときは、以下に説明する次のステップに移り、不一致のときは P C 3 0 0 から次のデータの受信を待機する待機状態に戻る。

## 【 0 0 5 7 】

双方の認証データが一致すると、今度は、R O M 1 3 C 内部のアルゴリズムで、乱数 A と、秘密鍵 2 と、2 つの公開鍵 1, 2 とが生成され、R O M 内のアルゴリズムで乱数 A と公開鍵 2 が公開鍵 1 で暗号化され、その公開鍵 1 で暗号化された乱数 A と公開鍵 2 が P C に送信されるとともに、公開鍵 1 自身も P C に送信される。生成された秘密鍵 2 は、R A M 1 2 C に格納される。また乱数 A および公開鍵 2 も R A M 1 2 C に格納される。

## 【 0 0 5 8 】

P C 3 0 0 は、暗号制御装置から公開鍵 1 と、その公開鍵 1 で暗号化された乱数 A と公開鍵 2 を受け取ると、暗号化された乱数 A と公開鍵 2 を公開鍵 1 で復号して平文の乱数 A と公開鍵 2 を取り出し、さらに乱数 B を生成し、公開鍵 1 による復号により取り出した乱数 A と新たに発生させた乱数 B を、上記のようにして取り出した公開鍵 2 で暗号化して暗号制御装置に送信する。この乱数 B は P C 内にも記憶しておく。

## 【 0 0 5 9 】

暗号制御装置では、それを受信すると、その受信データを R A M 1 2 C に記憶しておいた秘密鍵 2 で復号して乱数 A と乱数 B を取り出し、この取り出した乱数

Aと乱数Bのうちの乱数Aと、先に発生させてRAM12Cに格納しておいた乱数Aとが照合され、それらが一致した場合に、暗号制御装置は、そこに接続されたPCが暗号制御装置をアクセスする正当な権原を有する者であると認証する。不一致のときは、図8には示されていないがPCに向けて不一致であった旨連絡して待機状態に戻る。

【0060】

暗号制御装置で受信して復号化した乱数AとRAM12Cに格納しておいた乱数Aが一致すると、今度は公開鍵3を生成し、PC300から送信されて復号化された乱数Bと公開鍵3を、RAM12Cに格納しておいた公開鍵2で暗号化しPCに向けて送信する。公開鍵3はRAM12Cにも格納される。

【0061】

ここで、公開鍵3は、その公開鍵3で暗号化したデータをその公開鍵3自身で復号化することのできる鍵である。

【0062】

公開鍵2で暗号化された乱数Bと公開鍵3を受信したPCでは、受信したデータを公開鍵2で復号し、その復号化されたデータに含まれる乱数Bと公開鍵3のうちの乱数Bと、この乱数BはPCが自分で発生させたものであって、その発生させて記憶しておいた乱数Bとが照合され、それらが一致しているときは、自分が送受信している相手が、確かに自分がデータを送受信しようとしていた暗号制御装置である旨、認証する。

【0063】

これまでの間の、暗号制御装置におけるデータの復号化、暗号化は、全てROM13Cのアルゴリズムによりソフトウェア的に行なわれる。

【0064】

また、上記のようにして、そこに接続されたPCが暗号制御装置を正当にアクセスする権原を有する者であることが確認された後、暗号制御装置では暗号部15Cが動作可能状態とり、これ以降の暗号化、復号化は、暗号部15Cにより、ROM内のアルゴリズムを用いてソフトウェア的に行なうよりも高速に行なわれる。



## 【 0 0 6 5 】

また、図 7 に示す認証データの I / O 情報に応じて、その I / O 情報が I / O 部 1 4 C を動作可能状態に移行させることを指示していたときは I / O 部 1 4 C も動作可能状態となり、その I / O 情報が I / O 部 1 4 C を動作可能とする必要のないことを指示していたときは I / O 部 1 4 C は非動作状態にとどまる。こうすることにより I / O 部 1 4 C を動作させる必要のないときは I / O 部 1 4 C における電力消費が抑えられるとともに、暗号制御装置内部と外部との通信路を接続しておく機会の減少化を図り、一層の安全性が確保される。

## 【 0 0 6 6 】

上記のようにして P C と暗号制御装置との間での相互の認証が終了した後、P C から暗号制御装置に向けてコマンドが送信され、暗号制御装置からは P C に向けてそのコマンドに対するレスポンスが送信されるが、P C から暗号制御装置に送信されるコマンドは P C 側で公開鍵 3 で暗号化されて送信され、それを受け取った暗号制御装置側では、その暗号部 1 5 C により、R A M 1 2 C に格納しておいた公開鍵 3 を用いて復号化され、そのコマンドが実行される。

## 【 0 0 6 7 】

そのコマンドが実行された結果得られたコマンド結果（レスポンス）は暗号制御装置の暗号部 1 5 C で公開鍵 3 で暗号化されて P C に送信され、その暗号化されたレスポンスを受け取った P C 側では、そのレスポンスが公開鍵 3 で復号化されてレスポンスが取り出される。

## 【 0 0 6 8 】

以後、必要に応じて P C と暗号制御装置との間でこれと同様な通信が行なわれる。

## 【 0 0 6 9 】

ここで、上記のように、暗号制御装置には鍵生成手段が備えられており、この暗号制御装置では、その暗号制御装置自身で生成した鍵のみを用いて、復号化、暗号化が行なわれており、また秘密鍵は一切外出には出さないようになっている。また、認証により正当な通信相手ではないと判定されると暗号制御装置は待機状態に戻ってしまい動作しなくなり、また実質のデータ通信は認証により正当な

通信相手であることが確認された後に初めて行なわれる。このような構成により、データの秘密性、安全性が保たれ、データの不正な解読はほとんど不可能となる。

## 【 0 0 7 0 】

図 9 は、本発明の暗号制御装置の第 5 実施形態のブロック図である。図 6 に示す第 4 実施形態の暗号制御装置との相違点について説明する。

## 【 0 0 7 1 】

図 9 に示す第 5 実施形態の暗号制御装置には、図 6 に示す第 4 実施形態の暗号制御装置の I/O 部 1 4 C に相当する、3 つの I/O 部 1 4 1 D, 1 4 2 D, 1 4 3 D (I C C, U A R T 1, U A R T 2) が備えられている。これら 3 つの I/O 部 1 4 1 D, 1 4 2 D, 1 4 3 D を含む暗号制御装置 1 0 D を構成する各要素は 1 つの半導体素子 1 0 0 D に搭載されている。各 I/O 部 1 4 1 D, 1 4 2 D, 1 4 3 D には、それぞれ I C カード R/W 2 0 0、プリンタ (P R) 4 0 0、および遠隔通信用のモデム (M O D E M) 3 0 0 が接続されている。

## 【 0 0 7 2 】

図 9 は、図 8 に示す第 5 実施形態の暗号制御装置に向けて送信される認証データのデータ構造を示す図である。

## 【 0 0 7 3 】

この図 9 に示す認証データには、図 7 に示す認証データと比べ、コマンド情報が付加されている。

## 【 0 0 7 4 】

このコマンド情報は、3 つの I/O 部 1 4 1 D, 1 4 2 D, 1 4 3 D のうち、I/O 情報で指定される I/O 部を動作可能状態とする (O p e n) か、動作状態から非動作状態に戻す (C l o s e) か、あるいは、I/O 情報で指定される I/O 部を動作可能状態とするとともに他の動作可能状態の I/O 部があったときはそれを非動作状態に変更する (C h a n g e) かのいずれかのコマンドを示しており、P C からは、この認証データが暗号化されて暗号制御装置に送信され、暗号制御装置では受け取ったデータを復号化して平文の認証データを取り出し図 8 を参照して説明したようにして認証を行なった後、図 9 に示す 3 つの I/O

部 1 4 1 D, 1 4 2 D, 1 4 3 D を、その認証データ中のコマンド情報および I / O 情報に従って制御する。

【 0 0 7 5 】

こうすることにより、今回の処理に必要な I / O 部以外の I / O 部は非動作状態に保たれ、その電力消費が抑えられ、かつ、その I / O 部から出力されるデータが不正に解読されるおそれをなくしている。

【 0 0 7 6 】

さらに、図 9 に示す 3 つの I / O 部 1 4 1 D, 1 4 2 D, 1 4 3 D は、いずれもセキュリティレベルが、非動作状態（アクセス権無し）を含む複数段階に変更できるものであり、それに対応して、コマンド情報には、セキュリティレベルを 0 から 1 に変更する L e v e l U p 1 コマンド、セキュリティレベルを 1 から 2 に変更する L e v e l U p 2 コマンド、セキュリティレベルを 2 から 3 に変更する L e v e l U p 3 コマンド、およびセキュリティレベルを現在のセキュリティレベルから 1 つダウンさせる L e v e l D n コマンドを含ませることができる。

【 0 0 7 7 】

図 1 1 は、各セキュリティレベルごとのアクセス権の範囲と、各コマンドとの対応を示した図である。また、表 1 は、各セキュリティレベルごとのコマンドの作用を示したものである。

【 0 0 7 8 】

【表1】

	Level 1 UP1 マウント	Level 1 UP2 マウント	Level 1 UP3 マウント	Level 1 Dn マウント
セキュリティレベル 0	セキュリティレベル 1 へ	I/O-	I/O-	I/O-
セキュリティレベル 1	NOP	セキュリティレベル 2 へ	I/O-	セキュリティレベル 0 へ
セキュリティレベル 2	I/O-	NOP	セキュリティレベル 3 へ	セキュリティレベル 1 へ
セキュリティレベル 3	I/O-	I/O-	NOP	セキュリティレベル 2 へ

【0079】

このように、複数のセキュリティレベルを設けることにより、不必要なアクセ

スが防止され、安全性が一層向上する。

【 0 0 8 0 】

尚、図 9 に示す第 5 実施形態の暗号制御装置では、認証部 1 6 D は、P C 3 0 0 との接続部に用いられているが、モデム 5 0 0 を制御する I / O 部 1 4 3 D の内部に認証部を備えてもよい。こうすること、モデム 5 0 0 の先に P C 等を接続し、遠隔からこの暗号制御装置を動作させることができる。

【 0 0 8 1 】

図 1 2 は、本発明の暗号制御装置の第 6 実施形態を示す模式図である。

【 0 0 8 2 】

この図 1 2 の暗号制御装置 1 0 E には、S R A M 1 2 E のみ示されているが、この S R A M 1 2 E は、図 9 に示す R A M 1 2 D に代わるものであり、図 1 2 には図示省略されているが、図 1 2 に示す暗号制御装置は図 9 に示す各要素と同じ要素からなり、それらが 1 つの L S I チップ 1 0 0 E 上に搭載されている。

【 0 0 8 3 】

この図 1 2 には、L S I チップ 1 0 0 E に搭載された暗号制御装置 1 0 E が組み込まれた装置の筐体 6 0 0 が示されており、この筐体 6 0 0 内には、商用電源からの電力を暗号制御装置 1 0 E の S R A M 1 2 E に供給するメイン電源部 6 0 1、バッテリーに蓄積された電力を S R A M 1 2 E に供給するバッテリー電源部 6 0 2、この筐体 6 0 0 の分解や解体を検知する攻撃検知センサ 6 0 3、その攻撃検知センサ 6 0 3 からの信号を受けて筐体 6 0 0 が無理にこじ開けられようとしているなどの分解や解体を検出する異常検出器 6 0 4 が備えられている。尚、暗号制御装置 1 0 E の S R A M 1 2 E 以外の各要素へも電力が供給されるが、ここでは S R A M 1 2 E に注目しているため、他の要素およびそれら他の要素への電力供給経路等は図示省略されている。

【 0 0 8 4 】

ここで、攻撃検知センサ 6 0 3 からの信号により異常検出器 6 0 4 が筐体 6 0 0 の分解、解体などの異常を検知すると、その旨をメイン電源部 6 0 1 に通知し、メイン電源部 6 0 1 はそれを受けて S R A M 1 2 E を含む暗号制御装置 1 0 E への電力供給を強制的に遮断する。また、異常検出器 6 0 4 は、バッテリー電源部

6 0 2 から暗号制御装置 1 0 E への電力供給路を断ち切る。S R A M 1 2 E には、前述したようにして鍵が格納されるが、このよにして電力の供給が断たれると S R A M 1 2 E に格納された鍵やその他のデータは破壊されることになる。したがって不正に分解や解体を行なって鍵やその他のデータを不正に盗もうとしても失敗する結果となり、データの不正な漏洩が防止される。

## 【 0 0 8 5 】

尚、ここでは電力の供給を断つことにより鍵やその他のデータを破壊する例を示したが、この他にも、攻撃検知センサ 6 0 3 の信号あるいは異常検出器 6 0 4 の検出結果を暗号制御装置 1 0 E に割込信号として入力し、暗号制御装置では、その割込入力を受けて S R A M 1 2 E に無意味なデータを上書きをすることなどにより、ソフトウェア的に鍵やデータを破壊してもよい。

## 【 0 0 8 6 】

以下に、本発明の各種態様を付記する。

## 【 0 0 8 7 】

(付記 1) プログラムを実行する C P U と、該 C P U で実行されるプログラムが格納された R O M と、該 C P U でのプログラム実行中の作業領域として使用される R A M と、外部機器との間のデータの送受信を担う I / O 部と、暗号化されたデータの復号化および平文のデータの暗号化を担う暗号部とが 1 つの半導体素子上に形成されてなることを特徴とする暗号制御装置。

## 【 0 0 8 8 】

(付記 2) 前記 R A M が、暗号化されたデータを復号化するための秘密鍵を格納してなるものであり、

前記 R O M が、この暗号制御装置を使用する正当な権原を有する者を特定するデータを格納してなるものであって、

この暗号制御装置は、外部からデータが送信されてくるのを待つ待機モードと、動作が可能な動作可能モードとを有し、待機モードにあるときに外部から送信されてきた暗号化されたデータを前記 R A M に格納されている秘密鍵で復号化して平文のデータを生成し、該平文のデータと前記 R O M に格納されてなるデータとを照合し、これらのデータが符合するか否かに応じて、それぞれ、動作可能モ

ードに移行し、あるいは待機モードに戻るモード切換手段を有することを特徴とする付記 1 記載の暗号制御装置。

【 0 0 8 9 】

(付記 3) 前記 ROM は、前記動作可能モードで実行される複数のメインプログラムを格納してなるものであり、

この暗号制御装置は、前記待機モードにあるときに外部から送信されてきたデータに基づいて、前記動作可能モードで動作させる、前記複数のメインプログラムのうちのいずれか 1 つのメインプログラムを選択するメインプログラム選択手段を有することを特徴とする付記 2 記載の暗号制御装置。

【 0 0 9 0 】

(付記 4) 前記 1 つの半導体素子がさらに、この暗号制御装置との間で送受信されるデータに基づく情報処理を行なう外部の情報処理装置との間のデータの送受信を担うとともにデータを送信してきた者が正当な権原を有するものであるか否かを認証する認証部を搭載してなるものであることを特徴とする付記 1 記載の暗号制御装置。

【 0 0 9 1 】

(付記 5) データの暗号化、復号化に用いる鍵を生成する鍵生成手段を有し、この暗号制御装置は、該鍵生成手段で生成された鍵を用いてデータの暗号化および復号化を行なうものであることを特徴とする付記 1 記載の暗号制御装置。

【 0 0 9 2 】

(付記 6) 前記鍵生成手段は、秘密鍵と公開鍵とを生成し、公開鍵のみ外部に送信し、秘密鍵は前記 RAM に格納するものであることを特徴とする付記 5 記載の暗号制御装置。

【 0 0 9 3 】

(付記 7) 前記 RAM が、暗号化されたデータを復号化するための秘密鍵を格納してなるものであり、

前記 ROM が、この暗号制御装置を使用する正当な権原を有する者を特定するデータを格納してなるものであって、

前記認証部で受信された暗号化されたデータを前記 RAM に格納されている秘

密鍵で復号化して平文のデータを生成し、該平文のデータと前記 R O M に格納されてなるデータとを照合し、これらのデータが符合した場合に限り、前記 I / O 部を動作可能とする I / O 部制御手段を有することを特徴とする付記 4 記載の暗号制御装置。

【 0 0 9 4 】

(付記 8) 前記 1 つの半導体素子が、前記 I / O 部を複数搭載してなるものであって、

前記 I / O 部制御手段は、前記認証部で受信されたデータに基づいて、該データに応じた I / O 部のみ動作可能とするものであることを特徴とする付記 7 記載の暗号制御装置。

【 0 0 9 5 】

(付記 9) 前記 I / O 部は、複数のセキュリティレベルのうちの任意のセキュリティレベルの設定が自在なものであり、

前記 I / O 部制御手段は、前記認証部で受信されたデータに基づいて、前記 I / O 部を、該データに応じたセキュリティレベルに設定するものであることを特徴とする付記 7 記載の暗号制御装置。

【 0 0 9 6 】

(付記 1 0) 前記認証部は、外部の情報処理装置との間のデータの送受信を、モデムを介して行なうものであることを特徴とする付記 4 記載の暗号制御装置。

【 0 0 9 7 】

(付記 1 1) 異常の検知を受けて、前記 R A M に格納されている鍵を破壊するデータ破壊手段を有することを特徴とする付記 1 記載の暗号制御装置。

【 0 0 9 8 】

【発明の効果】

以上、説明したように、本発明によれば不正なデータの解読や漏洩が防止されデータの安全性が高度に保たれた暗号制御装置が実現する。

【図面の簡単な説明】

【図 1】



本発明の暗号制御装置の第 1 実施形態を示すブロック図である。

【図 2】

本発明の暗号制御装置の第 2 実施形態を示すブロック図である。

【図 3】

図 2 に示す第 2 実施形態における動作フローチャートである。

【図 4】

本発明の暗号制御装置の第 3 実施形態における、ROM 内部のプログラムの構造を示した模式図である。

【図 5】

図 4 にプログラム構造を示す第 3 実施形態における動作フローを示すフローチャートである。

【図 6】

本発明の暗号制御装置の第 4 実施形態を示すブロック図である。

【図 7】

認証データのデータ構造を示す図である。

【図 8】

本発明の暗号制御装置の第 5 実施形態のブロック図である。

【図 9】

図 8 に示す第 5 実施形態の暗号制御装置に向けて送信される認証データのデータ構造を示す図である。

【図 10】

認証データのデータ構造を示す図である。

【図 11】

各セキュリティレベルごとのアクセス権の範囲と、各コマンドとの対応を示した図である。

【図 12】

本発明の暗号制御装置の第 6 実施形態を示す模式図である。

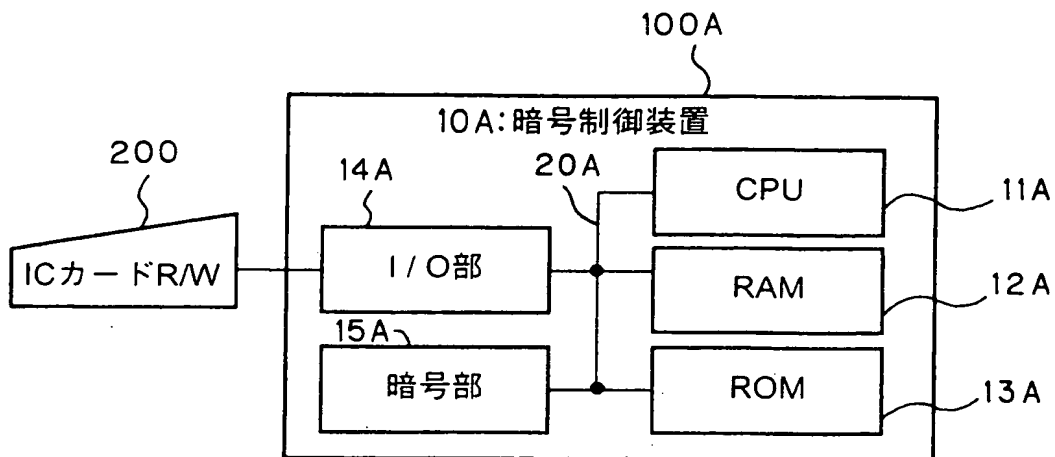
【符号の説明】

10A, 10B, 10C, 10D, 10E      暗号制御装置

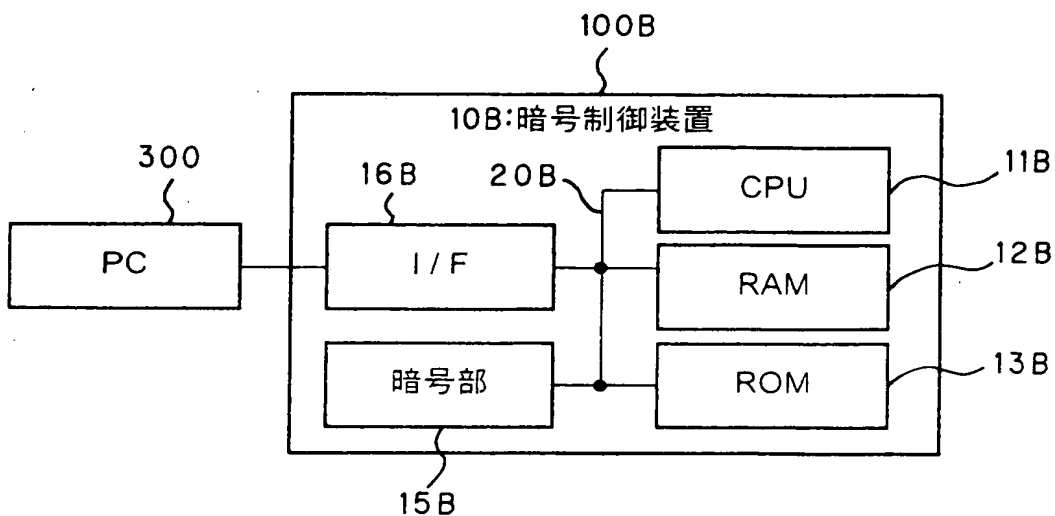
11A, 11B, 11C, 11D CPU  
12A, 12B, 12C, 12D RAM  
13A, 13B, 13C, 13D ROM  
14A, 14C I/O部  
15A, 15B, 15C 暗号部  
16B, 16C, 16D インタフェース部  
141D, 142D, 143D I/O部  
20A, 20B, 20C 内部バス  
100A, 100B, 100C, 100D, 100E 半導体素子  
200 ICカードR/W  
300 パーソナルコンピュータ(PC)  
400 プリンタ(PR)  
500 モデム  
600 筐体  
601 メイン電源部  
602 バッテリ電源部  
603 攻撃検知センサ  
604 異常検出器

【書類名】 図面

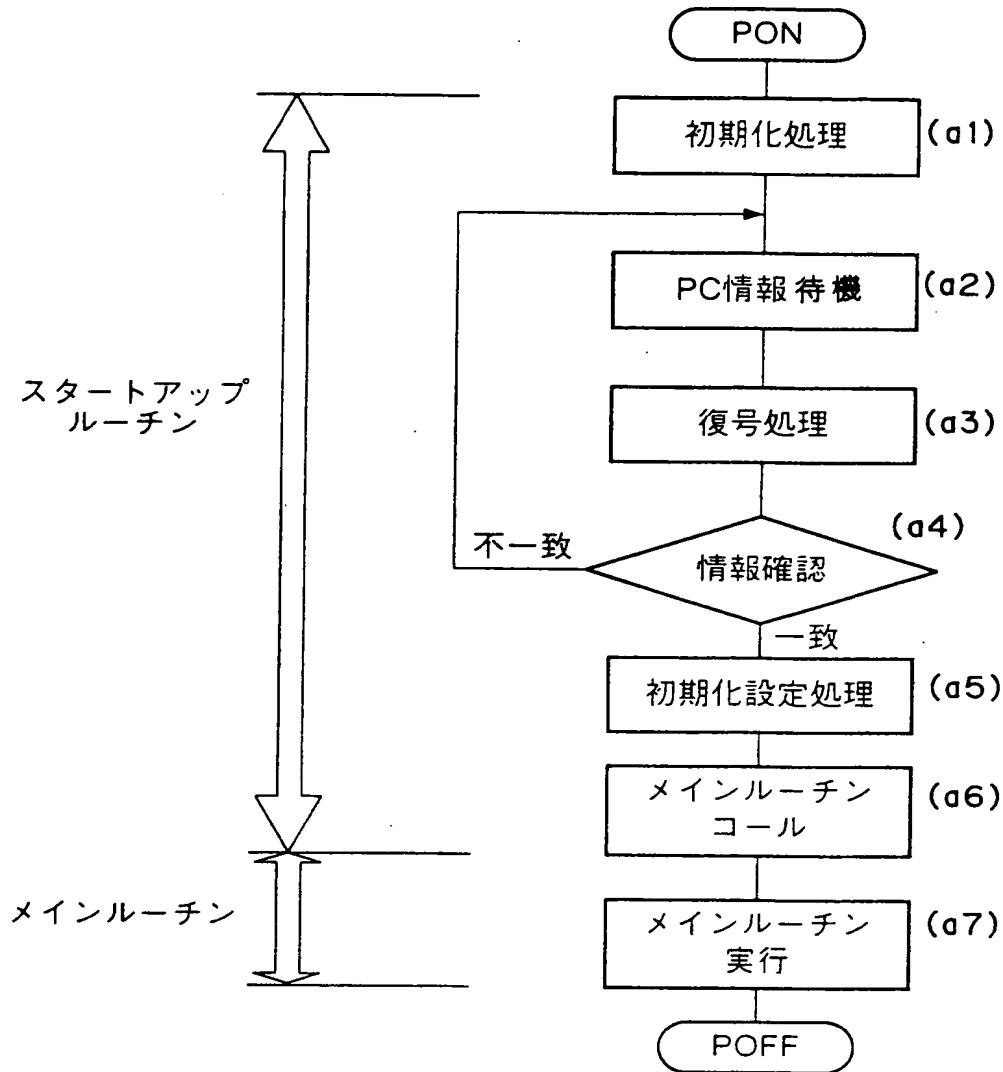
【図 1】



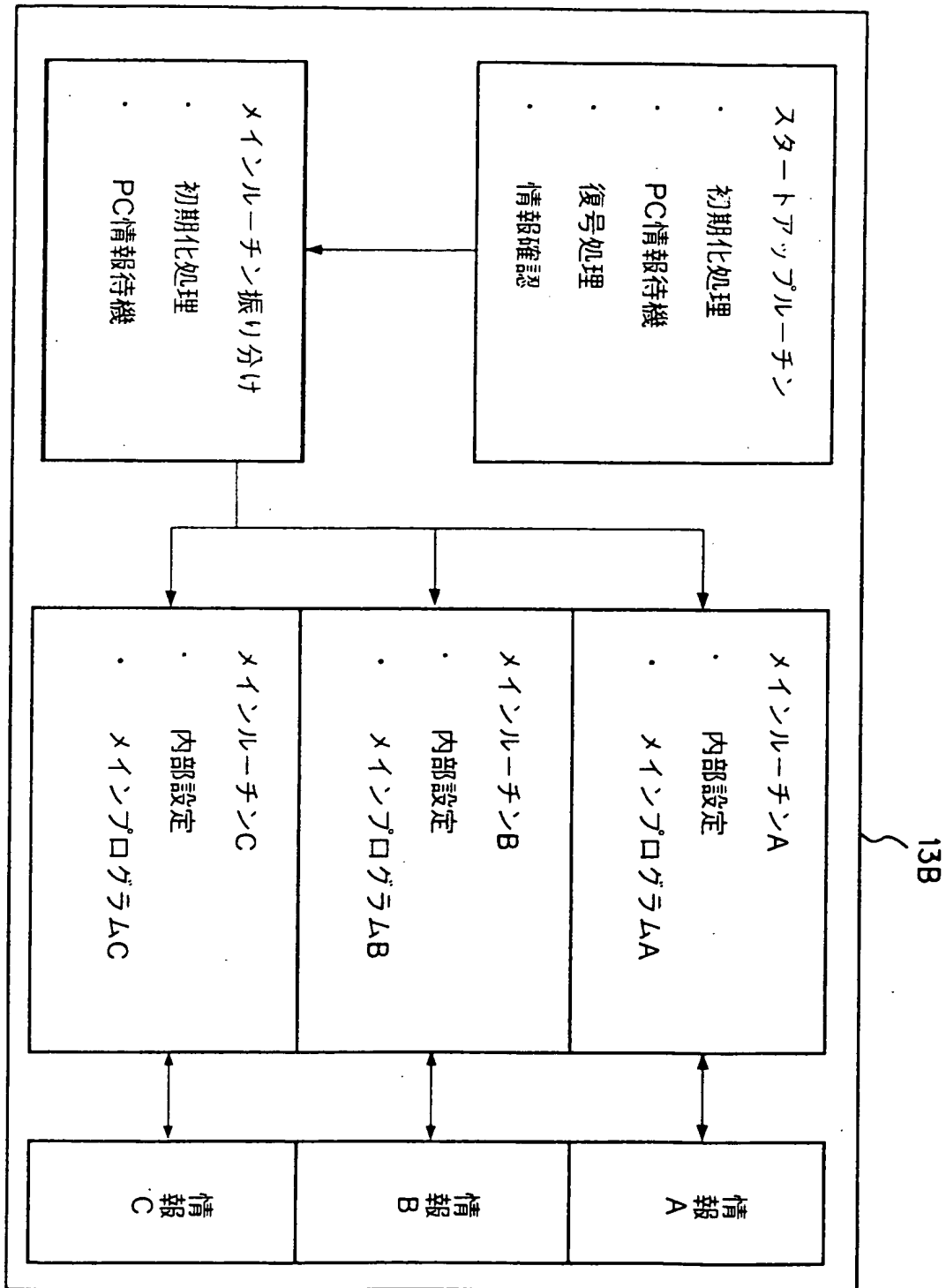
【図 2】



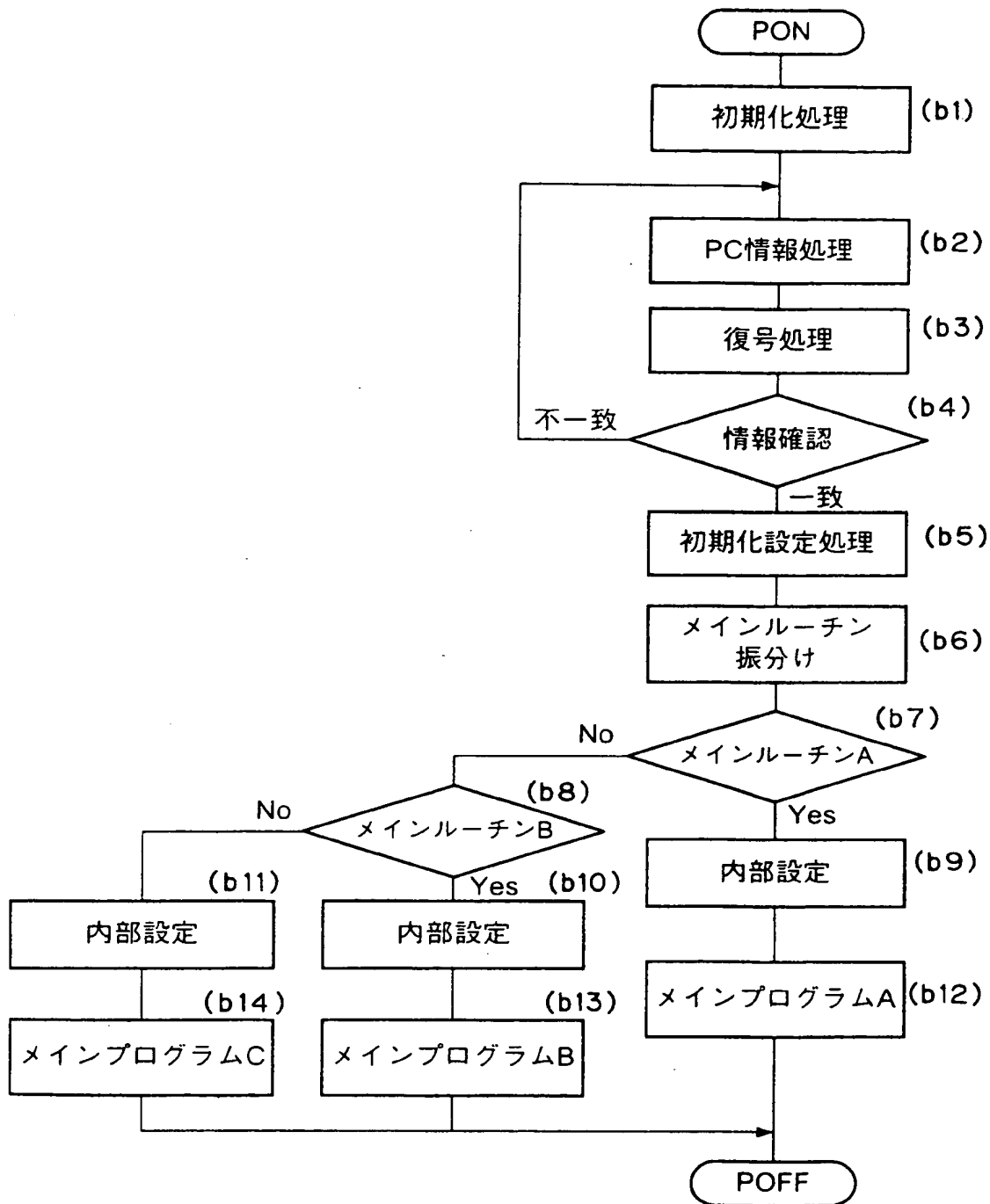
【図 3】



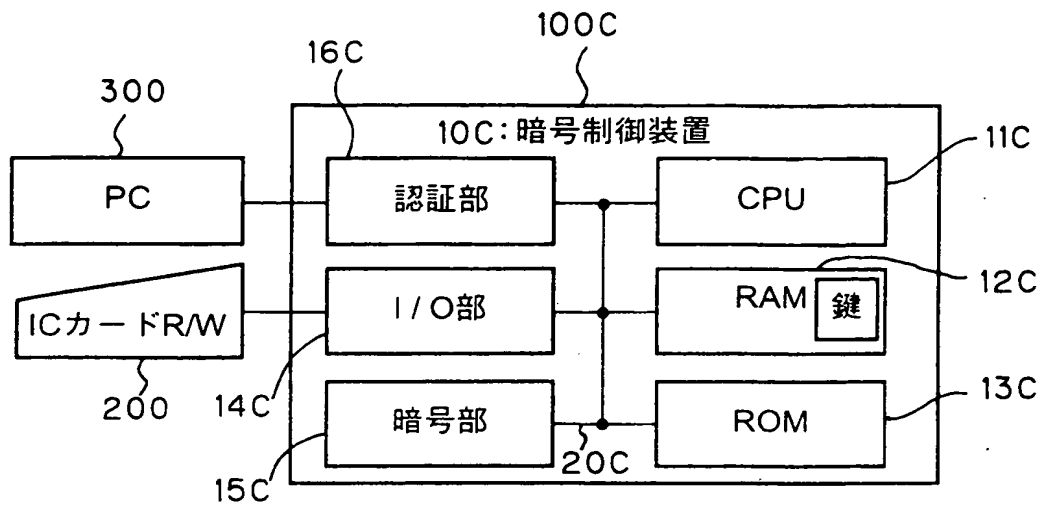
【図4】



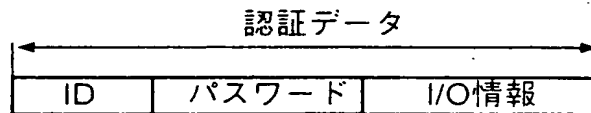
【図5】



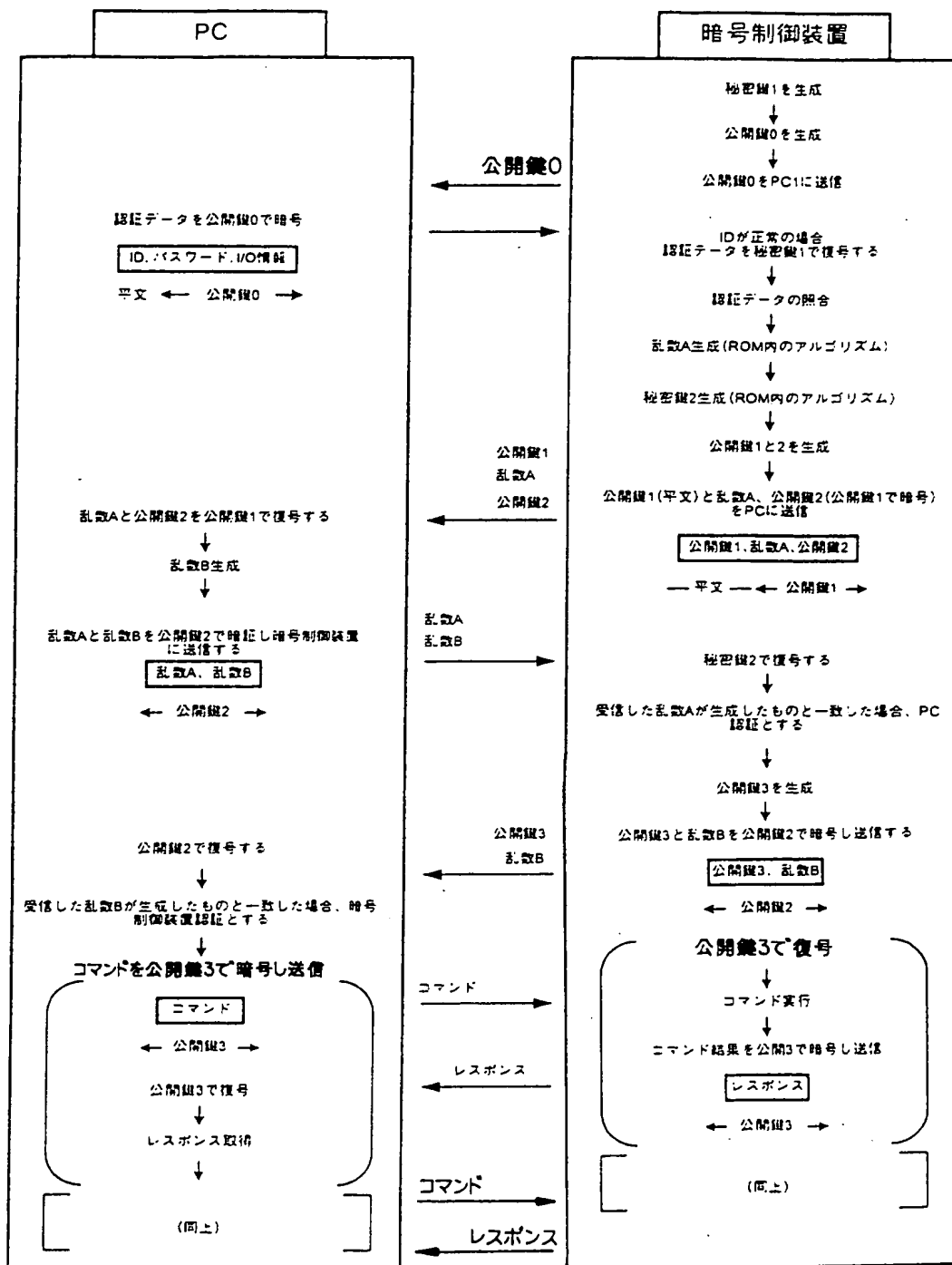
【図 6】



【図 7】

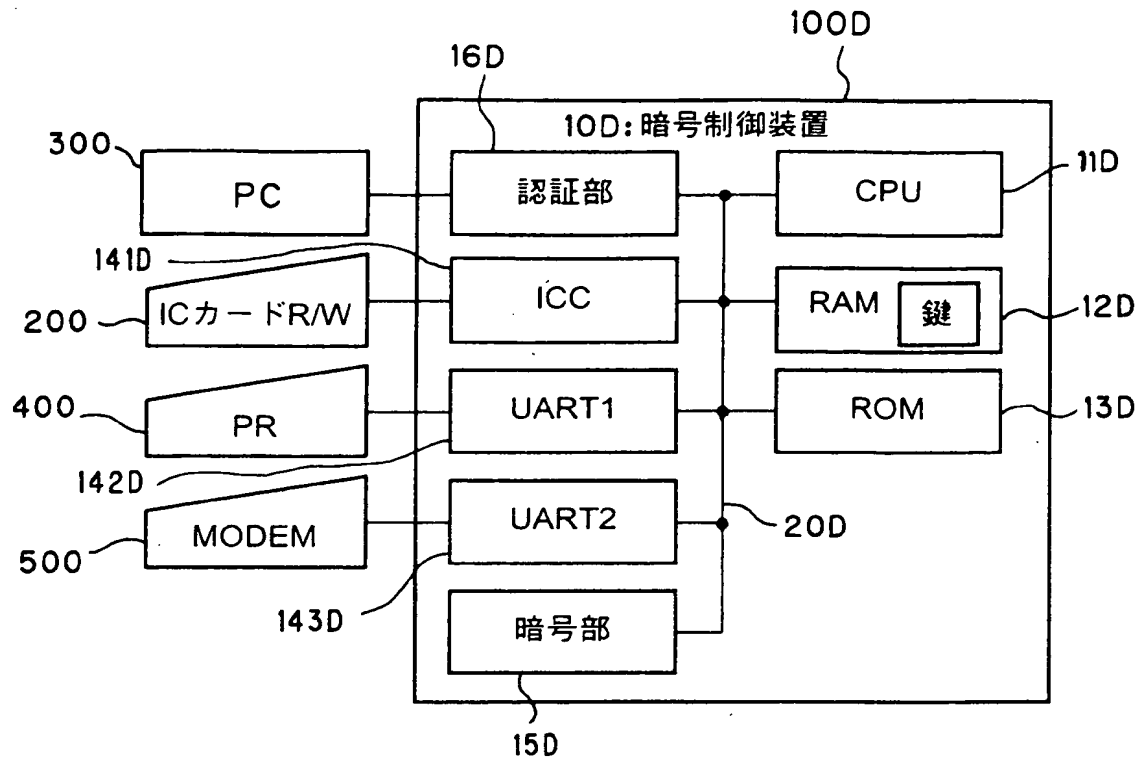


【図 8】

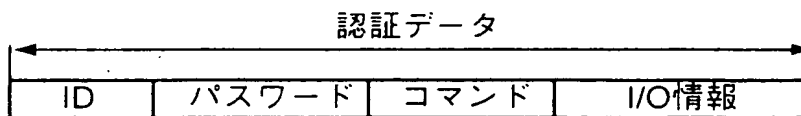




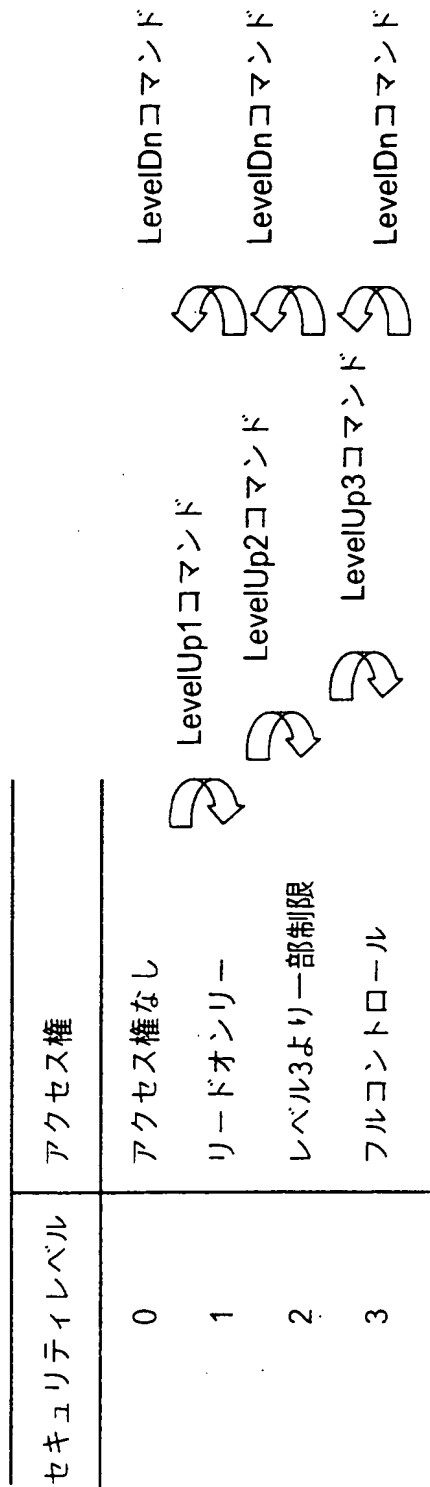
【図 9】



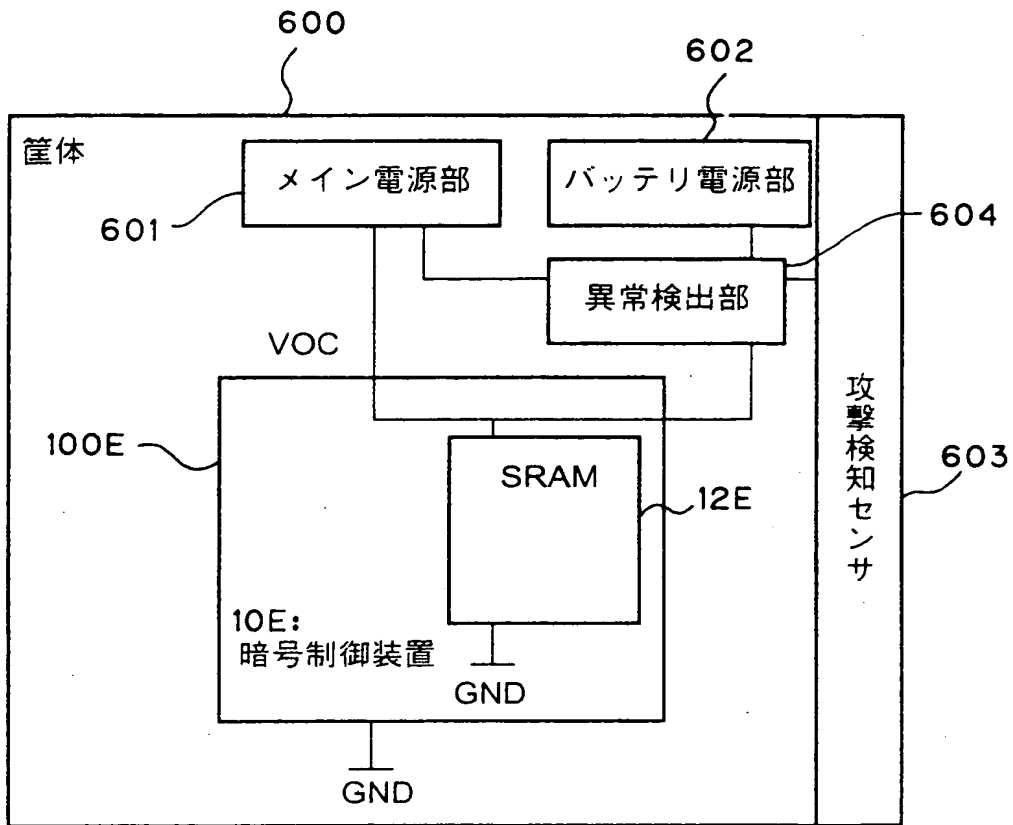
【図 1 0】



【図 11】



【図 1 2】



【書類名】 要約書

【要約】

【課題】本発明は、データの暗号化や復号化を担う暗号制御装置に関し、データの不正な解読や漏洩を防止し、データの安全性を向上させる。

【解決手段】プログラムを実行するCPU 11 Aと、CPUで実行されるプログラムが格納されたROM 13 Aと、CPUでのプログラム実行中の作業領域として使用されるRAM 12 Aと、外部機器との間のデータの送受信を担うI/O部 14 Aと、暗号化されたデータの復号化および平文のデータの暗号化を担う暗号部 15 Aとが1つの半導体素子上に形成されている。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日	1996年 3月26日
[変更理由]	住所変更
住 所	神奈川県川崎市中原区上小田中4丁目1番1号
氏 名	富士通株式会社